Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method of providing security in a gaming machine, the method comprising:

receiving a mechanical key in a lock within said gaming machine;

reading a first source of indicia from said key, wherein said first source of indicia comprises information or data specific to said lock;

reading a second source of indicia, wherein said second source of indicia comprises information specific to one or more users of said key;

authorizing a use of said key based on the readings of said first and second sources of indicia; and

permitting access to said key accessible environment.

[c2] 2. The method of claim 1, wherein said first source of indicia comprises one or more physical characteristics of said key.

[c3] 3. The method of claim 2, wherein said one or more physical characteristics of said key comprises at least one item selected from the group comprising a physical shape of said key, a groove arrangement of said key, and

at least a portion of an edge profile of said key.

[c4] 4. The method of claim 1, further including the step of:

capturing live data reflective of one or more parameters associated with any other step.

[c5] 5. The method of claim 1, wherein said information specific to one or more users of said key comprises biometric information with respect to said one or more users.

[c6] 6. The method of claim 5, wherein said biometric information comprises fingerprint related information.

[c7] 7. The method of claim 5, wherein said biometric information comprises at least one item selected from the group consisting of facial recognition, voice recognition, and retinal scan.

[c8] 8. The method of claim 1, wherein said information specific to one or more users of said key is contained within one or more authorized user IDs.

[c9] 9. The method of claim 8, further including the step of:

revoking a previously authorized user ID.

[c10] 10. The method of claim 1, further including the step of:

restricting access to said key accessible environment selectively based on one or more additional factors.

[c11] 11. A method of providing security in a key accessible environment, the method comprising:

receiving a key in a lock;

reading a first source of indicia from said key, wherein said first source of indicia comprises information or data specific to said lock;

reading a second source of indicia, wherein said second source of indicia comprises information specific to one or more users of said key;

authorizing a use of said key based on the readings of said first and second sources of indicia; and

permitting access to said key accessible environment.

[c12] 12. The method of claim 11, wherein said first source of indicia comprises one or more physical characteristics of said key.

[c13] 13. The method of claim 12, wherein said one or more physical characteristics of said key comprises at least one item selected from the group comprising a physical shape of said key, a groove arrangement of said key, and at least a portion of an edge profile of said key.

[c14] 14. The method of claim 11, further including the step of:

capturing live data reflective of one or more parameters

associated with any other step.

[c15] 15. The method of claim 11, wherein said information specific to one or more users of said key comprises biometric information with respect to said one or more users.

[c16] 16. The method of claim 15, wherein said biometric information comprises fingerprint related information.

[c17] 17. The method of claim 15, wherein said biometric information comprises at least one item selected from the group consisting of facial recognition, voice recognition, and retinal scan.

[c18] 18. The method of claim 11, wherein said information specific to one or more users of said key is contained within one or more authorized user IDs.

[c19] 19. The method of claim 18, further including the step of:

revoking a previously authorized user ID.

[c20] 20. The method of claim 11, wherein said information specific to one or more users of said key involves the use of an active PIN authentication.

[c21] 21. The method of claim 11, further including the step of:

restricting access to said key accessible environment based on one or more additional factors.

[c22] 22. The method of claim 21, wherein one additional factor includes the use of specified time periods.

[c23] 23. The method of claim 11, wherein said key accessible environment comprises a gaming machine.

[c24] 24. An apparatus, comprising:

a key accessible environment; and

an electromechanical lock securing said key accessible environment, wherein said electromechanical lock is adapted to deny access to said key accessible environment unless a mechanical key having a correct first source of indicia is inserted into the lock and an authorization signal is provided based upon the verification of a correct second source of indicia with respect to the user of said mechanical key.

[c25] 25. The apparatus of claim 24, wherein said first source of indicia comprises at least one item selected from the group comprising a physical shape of said key, a groove arrangement of said key, and at least a portion of an edge profile of said key.

[c26] 26. The apparatus of claim 24, wherein said second source of indicia comprises biometric information with

respect to said user of said mechanical key.

[c27] 27. The apparatus of claim 26, wherein said biometric information comprises fingerprint related information.

[c28] 28. The apparatus of claim 24, wherein second source of indicia involves the use of an active PIN authentication.

[c29] 29. An apparatus, comprising:

a locking means for securing a key accessible environment, wherein said locking means is adapted to deny access to said key accessible environment unless two separate sources of indicia are read and confirmed by said locking means.

[c30] 30. The apparatus of claim 29, further including an opening means for unlocking said locking means, said opening means having a first source of indicia comprising information or data specific to said locking means and a second source of indicia comprising information specific to one or more users of said opening means.

[c31] 31. A gaming machine, comprising:

at least one key accessible region; and

an electromechanical lock securing said at least one key accessible region, wherein said electromechanical lock is adapted to deny access to said key accessible region unless a mechanical key having a correct

first source of indicia is inserted into the lock and an authorization signal is provided based upon the verification of a correct second source of indicia with respect to the user of said mechanical key.

[c32] 32. The gaming machine of claim 31, wherein said first source of indicia comprises at least one item selected from the group comprising a physical shape of said key, a groove arrangement of said key, and at least a portion of an edge profile of said key.

[c33] 33. The gaming machine of claim 31, wherein said second source of indicia comprises biometric information with respect to said user of said mechanical key.

[c34] 34. The gaming machine of claim 33, wherein said biometric information comprises fingerprint related information.

[c35] 35. The gaming machine of claim 31, wherein second source of indicia involves the use of an active PIN authentication.

[c36] 36. A method of providing security in a gaming machine, the method comprising:

receiving a key in a lock;

reading a user-based source of indicia, wherein said user-based source of indicia comprises information

specific to one or more users of said key;

authorizing a use of said key based on an affirmative reading of said user-based source of indicia; and

permitting access to said gaming machine or a component thereof in the event that said key is a correct key for said lock.

[c37] 37. The method of claim 36, further including the step of:

capturing live data reflective of one or more parameters associated with any other step.

[c38] 38. The method of claim 36, wherein said information specific to one or more users of said key comprises biometric information specific to said one or more users.

[c39] 39. The method of claim 38, wherein said biometric information comprises fingerprint related information.

[c40] 40. The method of claim 38, wherein said biometric information comprises at least one type of information selected from the group consisting of fingerprint, facial recognition, voice recognition, and retinal scan information.

[c41] 41. A universal key security system, comprising:

at least one computer server; and

one or more gaming machines in communication

with said at least one computer server, wherein at least one of said one or more gaming machines comprises an electromechanical lock securing at least one region of said gaming machine,
wherein said electromechanical lock is adapted to deny access to said at least one region of said gaming machine unless a key having a correct first source of indicia is inserted into the lock and an authorization signal is provided based at least in part upon the verification of a correct second source of indicia with respect to the user of said mechanical key.

[c42] 42. The universal key security system of claim 41, wherein said information specific to one or more users of said key comprises biometric information with respect to said one or more users.

[c43] 43. The universal key security system of claim 41, further including a database in communication with said at least one computer server.

[c44] 44. The universal key security system of claim 43, wherein said database comprises at least one file containing information related to an authorized user of said universal key security system.

[c45] 45. The universal key security system of claim 41, wherein said at least one computer server is adapted to capture live data associated with an attempt to access said at least one region of said gaming machine secured by said electromechanical lock.

[c46] 46. The universal key security system of claim 41, wherein said authorization signal is provided at least in part through the use of said at least one computer server.

[c47] 47. The universal key security system of claim 41, wherein said verification of a correct second source of indicia with respect to the user of said mechanical key is accomplished at least in part through use of said at least one computer server.